NPS-CAG-14-010

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Trusted Computing Exemplar: Trusted Distribution Plan – Preliminary Design

by

Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen

12 December 2014

Approved for public release; distribution is unlimited

Prepared for: United States Navy, OPNAV N2/N6

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route
President

Douglas A. Hensler
Provost

The report entitled "Trusted Computing Exemplar: Trusted Distribution Plan – Preliminary Design" was prepared for United States Navy, OPNAV N2/N6 and funded in part by United States Navy, OPNAV N2/N6.

Further distribution of all or part of this report is authorized.

This report was prepared by:

Paul C. Clark
Research Associate

Cynthia E. Irvine
Distinguished Professor

Thuy D. Nguyen
Research Associate

Reviewed by:

Cynthia E. Irvine, Chair
Cyber Academic Group

Released by:

Jeffrey D. Paduan
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved* OMB No. 0704-0188

1. REPORT DATE ***(DD-MM-YYYY)*** 12-12-2014	**2. REPORT TYPE** Technical Report	**3. DATES COVERED** ***(From-To)*** Nov 2013 to Nov 2014

4. TITLE AND SUBTITLE Trusted Computing Exemplar: Trusted Distribution Plan – Preliminary Design	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Paul C. Clark, Cynthia E. Irvine, and Thuy D. Nguyen	**5d. PROJECT NUMBER** W4C05
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER** NPS-CAG-14-010
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Rhonda Onianwa OPNAV, N2N6 F13 rhonda.onianwa@navy.mil LT David Rivera OPNAV, N2/N6F1 david.j.rivera4@navy.mil	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for pubic release; distribution is unlimited

13. SUPPLEMENTARY NOTES
The view expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense of the U.S. Government.

14. ABSTRACT

This document describes the Life Cycle Management Plan for the development of a high assurance secure product. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional.

This document describes the policy and high-level processes for the distribution of the TCX product to external users. This document is driven by the TCX Life Cycle Management Plan (LCMP), the Configuration Management Plan, and the Quality Assurance Plan. This document provides the framework for the Integration Procedures and the Delivery Procedures identified in the LCMP. Some of the concepts described in this document were developed in a student's Masters thesis.

This is a preliminary design for product distribution; it has not been tested with a product actually distributed to end-users.

.

15. SUBJECT TERMS
Machinery control systems, MCS, life cycle security, high assurance, system security, trustworthy systems

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UU	15	Cynthia E. Irvine
					19b. TELEPHONE NUMBER ***(include area code)*** (831) 656 2461

THIS PAGE INTENTIONALLY LEFT BLANK

CYBER ACADEMIC GROUP
NAVAL POSTGRADUATE SCHOOL

NPS-CAG-14-010

Trusted Computing Exemplar: Trusted Distribution Plan – Preliminary Design

Paul C. Clark
Cynthia E. Irvine
Thuy D. Nguyen

December 2014

ATTRIBUTION REQUEST

December 2014

The Cyber Academic Group (CAG) and the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS) wish to facilitate and encourage the development of highly robust security systems.

To further this goal, the NPS CAG and NPS CISR ask that any derivative products, code, writings, and/or other derivative materials, include an attribution for NPS CAG and NPS CISR. This is to ensure that the public has a full opportunity to direct questions about the nature and functioning of the source materials to the original creators.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the following organizations for providing support toward the development of this work: OPNAV N2/N6 F1.

The material presented here builds upon work supported in previous years by the Office of Naval Research.

A portion of the material presented here is based upon work supported by the National Science Foundation under Grant No. CNS-0430566 and CNS-0430598. This document does not necessarily reflect the views of the National Science Foundation.

Table of Contents

Table of Figures

.

1 Introduction

This document has been written in support of a research project to publicly demonstrate and document how a high assurance product can be developed and distributed. A high assurance product is one for which its users have a high level of confidence that its security policies will be enforced continuously and correctly. Such products are constructed so that they can be analyzed for these characteristics. Lifecycle activities ensure that the product reflects the intent to ensure that the product is trustworthy and that vigorous efforts have been made to ensure the absence of unspecified functionality, whether accidental or intentional.

This document describes the policy and high-level processes for the distribution of the TCX product to external users. This document is driven by the TCX Life Cycle Management Plan (LCMP) [1], the Configuration Management Plan [2], and the Quality Assurance Plan [3]. This document provides the framework for the Integration Procedures and the Delivery Procedures identified in the LCMP. Some of the concepts described in this document were developed in a student's Masters thesis [4].

This is a preliminary design for product distribution; it has not been tested with a product actually distributed to end-users.

2 The Approach to Trusted Distribution

An important aspect of high assurance is the verification that the product that was received by the customer is the product that was built by the developer. Distribution can be assured through the proper use of a PKI, as shown in Figure 1.

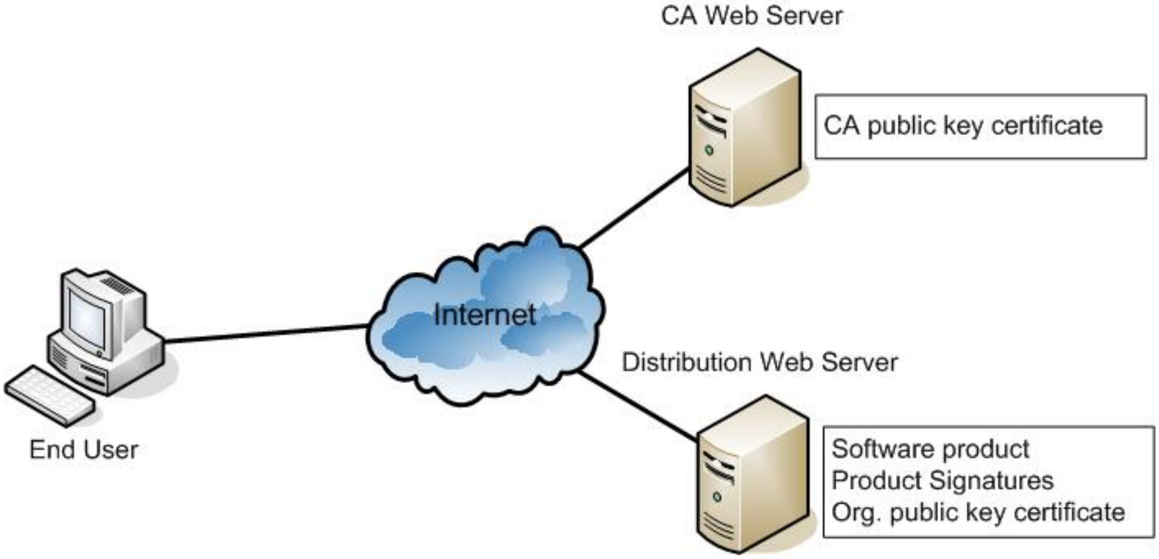

Figure 1 Independent Channels

The software product shall be signed with a physically protected private key. The complementary public key shall be signed by a recognized Certificate Authority (CA)

The CA public key shall be used to verify the integrity and validity of the software organization's public key. The organization's public key together with the product signatures are then used to verify the integrity of the distributed software product.

Rationale: Public key certificates must be signed by a recognized authority, i.e., they shall not be self-signed. Self-signed certificates would provide an opportunity for certificate forgery and therefore an opportunity to replace all or part of the distributed items without detection.

3 From Creation to Distribution

Figure 2 shows an expanded view of the flow described in [3], showing the additional high-level steps for distribution.

When the CCB approves a submission, the CM staff imports the material into the CM Repository [2]. As a separate action, the Project Manager must also approve the public release of material. The Project Manager compiles a list of the items to be publicly released on a Releasable Items List (RIL), which constitute the product. The RIL is then given to the CM staff.

A person acting as an assigned Release Agent (RA) will request material from CM. CM will comply as long as the requested items are on the RIL and the person is designated as an RA by the Project Manager. The requested items are cryptographically signed by CM when the RA requests the items. A record of all signatures is maintained by the CM staff. The items and the signatures are given to the RA. Key pairs may be generated for the RA if it is determined that post-CM packages need to be created. The RA will arrange to have the requested items imported into the TCX web server, along with their signatures.

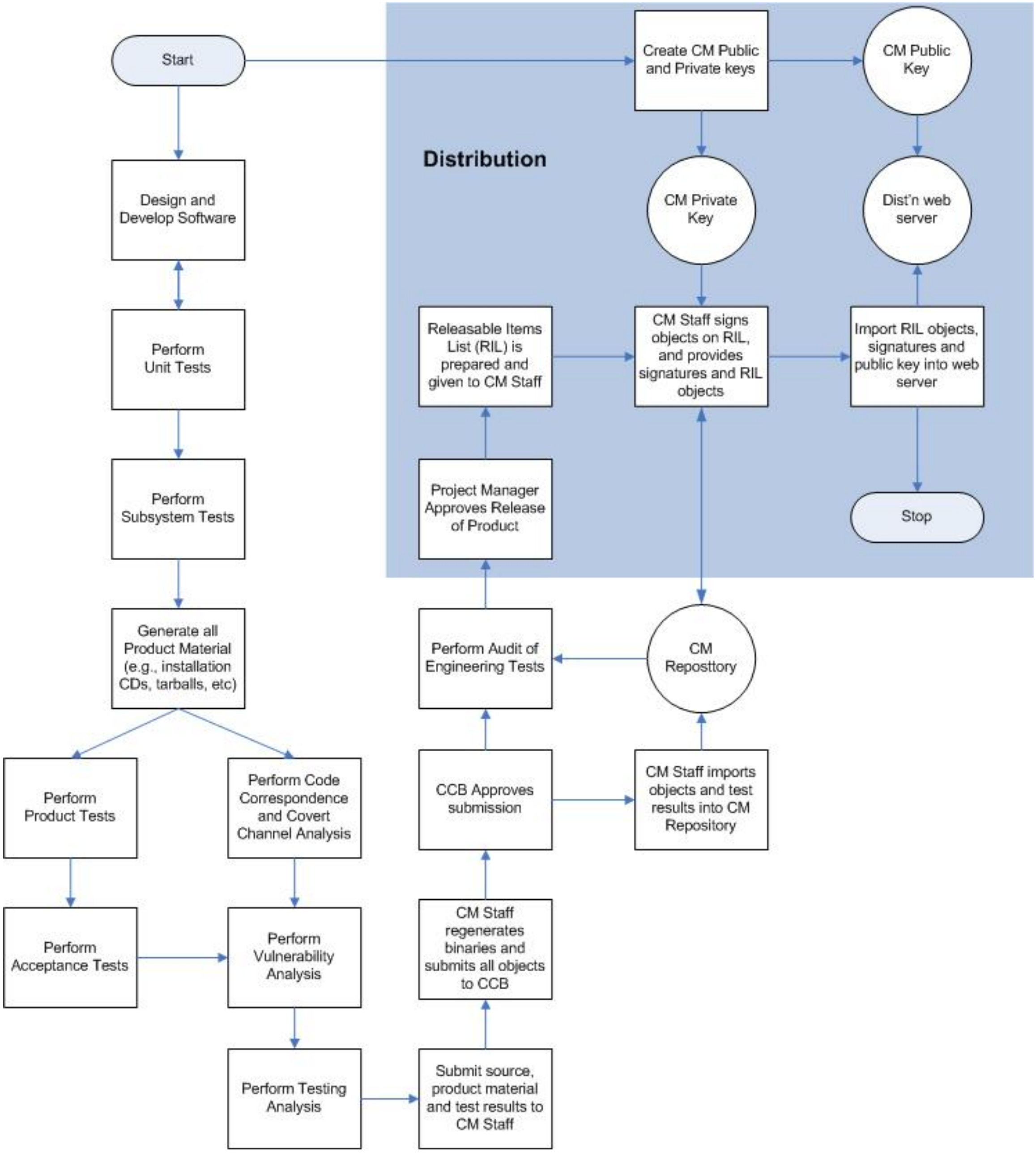
Start
Create CM Public and Private keys
CM Public Key
Distribution
Design and Develop Software
CM Private Key
Dist'n web server
Perform Unit Tests
Releasable Items List (RIL) is prepared and given to CM Staff
CM Staff signs objects on RIL, and provides signatures and RIL objects
Import RIL objects, signatures and public key into web server
Perform Subsystem Tests
Project Manager Approves Release of Product
Stop
Generate all Product Material (e.g., installation CDs, tarballs, etc)
Perform Audit of Engineering Tests
CM Reposttory
Perform Product Tests
Perform Code Correspondence and Covert Channel Analysis
CCB Approves submission
CM Staff imports objects and test results into CM Repository
Perform Acceptance Tests
Perform Vulnerability Analysis
CM Staff regenerates binaries and submits all objects to CCB
Perform Testing Analysis
Submit source, product material and test results to CM Staff

Figure 2 The Flow to Distribution

4 Notification Setup During Distribution

In the event that security-relevant bugs are found after a product has been distributed, then it shall be necessary to inform the users of such bugs and the steps being taken to remediate them. Direct notification is challenging because of the nature of an anonymous web server download. However, when a user is about to download the product from the web server, they shall be given the opportunity to optionally register an e-mail address for such bug notifications. In addition, the web server should provide information about reported bugs.

References

[1] P.C. Clark, C. E. Irvine, T. Levin, and T. D. Nguyen, “Trusted Computing Exemplar: Life cycle management plan,” Naval Postgraduate School, Monterey, CA, Tech. Rep. NPS-CAG-14-002, Dec. 2014.

[2] P.C. Clark, C. E. Irvine, T. Levin, T. D. Nguyen, and Daniel Warren, “Trusted Computing Exemplar: Configuration management plan,” Naval Postgraduate School, Monterey, CA, Tech. Rep. NPS-CAG-14-003, Dec. 2014.

[3] P.C. Clark, C. E. Irvine, T. Levin, and T. D. Nguyen, “Trusted Computing Exemplar: Quality Assurance Plan,” Naval Postgraduate School, Monterey, CA, Tech. Rep. NPS-CAG-14-009, Dec. 2014.

[4] D. R. Kane Jr., “Web-based dissemination system for the Trusted Computing Exemplar project,” M.S. thesis, CS Dept., Naval Postgraduate School, Monterey, CA, 2005.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   Ft. Belvoir, Virginia

2. Dudley Knox Library, Code 013 2
   Naval Postgraduate School
   Monterey, California 93943

3. Research Sponsored Programs Office, Code 41 1
   Naval Postgraduate School
   Monterey, California 93943

4. Paul C. Clark 1
   Naval Postgraduate School
   Monterey, California 93943

5. Dr. Cynthia E. Irvine 1
   Naval Postgraduate School
   Monterey, California 93943

6. Thuy D. Nguyen 1
   Naval Postgraduate School
   Monterey, California 93943